# METHOD AND APPARATUS FOR CONTROLLING THE DISTRIBUTION OF DIGITALLY ENCODED DATA IN A NETWORK

## RELATED APPLICATIONS

**[0001]** The present application claims priority under 35 U.S.C. § 119 of Provisional Patent Application Serial Number 60/387,054 entitled "Proposal on the Use of the BPDG Broadcast Flag" filed on June 7, 2002.

## FIELD OF THE INVENTION

**[0002]** The present invention relates to communication systems generally and, more particularly, to a system and method for protecting unauthorized distribution of content to a remote network location.

## BACKGROUND OF THE INVENTION

**[0003]** Content creators and providers, such as movie studios, production companies and service providers (ISPs), have a need for protecting their investment, for example, movies, programming, services, software, and the like. Such content has typically found its way to the consumer through terrestrial broadcasts, premium programming, cable or satellite channels, pay-per-view events, and retail sales and rentals of videocassettes.

**[0004]** In terrestrial broadcasts, program content is transmitted in digital format to an access device such as a digital receiver. The nature of digital storage and transmission allows endless generations of copies to be produced with the same quality as the original master. Furthermore, unless the signal is encrypted, the received content may be easily copied and/or forwarded to additional products or devices not intended or authorized to receive such content. Moreover, products with digital outputs allow for the convenience of networked systems and higher quality recording and re-transmission of data. A home network, which receives content for display and storage, must now also protect content against illegal copying or distribution.

**[0005]** It has been proposed that a broadcast flag (BF) be carried in a digital signal such as a video broadcast stream, for the purpose of identifying that the digitally encoded data (such as video content) shall not be transmitted outside of the receiving device's own network. As used herein, the term content includes the digital signal, or the digitally encoded data, that

is used to carry the program content. The flag may be carried in the PMT/EIT field of an MPEG-2 transport stream, for example, as a field comprising one or more bits. Currently, however, no mechanism exists for implementing how a network such as a home network should honor the flag so that content is not transmitted outside of the network.

**[0006]** One possible solution is to add additional flags into other portions of the digital signal, such as an Ethernet header, to signify to a router, cable modem and the like, that the content should not be forwarded to the outside world. Another proposal would require the use of only protected (encrypted data) interfaces such as IEEE 1394 with 5C or DVI with HDCP. However, such implementations have the disadvantage of requiring costly changes to the infrastructure of existing (as well as future) home networks. Such infrastructure changes would significantly impede the trend of customers using their home network to distribute content to other electronic devices within their own home, thereby stifling a very promising market for home user electronic devices and content distribution within a home network.

## SUMMARY OF THE INVENTION

**[0007]** The present invention provides a method for controlling distribution of digitally encoded content from an access device attached to a network to another device outside the network, the access device receiving a digital signal representative of program content, the digital signal having an authorization field indicative of a first transport mode authorizing the distribution of the content outside the network, and of a second transport mode inhibiting the distribution of the content outside the network. The method comprises the steps of receiving location information of a router on the network that is used for routing content to devices outside the network; receiving destination data indicative of location information associated with a destination device to which the access device intends to distribute the content; determining whether the destination device is outside the network based on the router location information and the received destination data; examining the authorization field and, controlling the distribution of the content in response to the determination of whether the device is outside the network and whether the transport mode authorizes or inhibits the distribution of the content outside the network.

**[0008]**

In another aspect, the present invention also provides a device coupled to a network for distributing content to at least another device, the access device receiving a digital signal

representative of program content, the digital signal including an authorization field indicative of a first transport mode wherein authorizing distribution of the digital signal is authorized outside the network, and a second transport mode inhibiting distribution of the digital signal outside the network. The device comprises memory having stored therein computer code for executing a send operation for transmitting data on the network; a processor for controlling data receiving and transmitting operations of the device, the processor including data storage means for storing address information of devices connected to the network; and data interface means, coupled to the network, for receiving data from devices attached to the network, and for distributing the digital signals on the network, wherein the processor inhibits transmission of the digital signal on the network in response to a determination that the device is outside the network and that the authorization field is indicative of the second transport mode, otherwise, the processor enables transmission of the digital signal on the network.

## BRIEF DESCRIPTION OF THE DRAWINGS

**[0009]** Figure 1 is a block diagram of a home network system embodying an aspect of the present invention.

**[0010]** Figure 2 is an exemplary block diagram illustrating major functional components associated with the propagation and reception of packets representative of video frame transport stream information.

**[0011]** Figure 3 is a block diagram of a transport stream.

**[0012]** Figure 4A is an exemplary illustration of PAT and PMT linkage containing a broadcast flag authorization field within a transport stream.

**[0013]** Figure 4B is an exemplary illustration of an EIT containing a broadcast flag authorization field within a transport stream.

**[0014]** Figure 5 is a flow chart illustrating an exemplary method of operation according to an embodiment of the present invention.

## DETAILED DESCRIPTION

**[0015]** Referring now to FIG. 1, there is shown a home network system 10 comprising a plurality of access devices 20, 30, 40, 50, 60 coupled via a home network such as Ethernet

network 70 through switch 80 to router/gateway device 90. Home router 90 bridges multiple external service providers (e.g. internet 100) and remote devices (e.g. electronic device 110 or optional modem 95) outside the home network to enable communications with home network 70. For example, router 90 is capable of receiving and forwarding media feeds from terrestrial broadcast sources, satellite broadcasts, cable and the like, via a corresponding interface (e.g. terrestrial broadcast I/F, satellite I/F, asynchronous digital subscriber line I/F, etc.). It is understood that the router 90 is capable of IP routing and transport stream routing of data packets via an appropriate protocol, such as MPEG-2 for example, to various consumer electronic devices both inside and outside the home network.

**[0016]** In the exemplary embodiment depicted in FIG. 1, router 90 is a conventional router device having a mapping table for mapping device IP addresses to physical addresses for routing data into and/or outside of the home network. The access devices 20-60 located within the home network may be any one of a number of consumer electronic devices, including but not limited to servers, digital televisions and monitors, MP3 and DVD devices, printers and print serves, Personal computers (PCs) and the like. In the exemplary configuration of FIG. 1, device 20 is a Television device such as an HDTV coupled via bus 25 to media renderer device 30 (e.g. Replay 4000). The exemplary home network system 10 shown in FIG. 1 further includes media server 40, MP3 network player 50 and personal computer (PC) 60. Each of these devices has an associated IP address, physical address and subnet mask, as is understood in the art.

**[0017]** Router 90 is operable to receive a digital signal such as an MPEG-2 open terrestrial broadcast signal and forward the signal to the appropriate receiving device on the home network. Note that other such terrestrial broadcast signals may also be received and processed for transfer to the home network 10, such as MPEG-1, MPEG-4, JPEG, and the like.

**[0018]** The receiving/access devices within the home network are configured with appropriate hardware and/or software functionality to receive and decode packetized data such as MPEG-2 transport streams containing audio/video/data content. Compression algorithms at the source of the broadcast operate to reduce the required bandwidth for the transmission medium and yet maintain reasonable video quality at the receiver.

**[0019]** FIG. 2 is an exemplary illustration of an arrangement whereby video frame content is transmitted via packets through Ethernet packet network 70 illustrated in FIG. 1.

Each video frame produced by a standard source (not shown), as exemplified by frame 210 serving as the input to a transmitter 201, is compressed by encoder 220 with reference to an encoding program stored in program memory 225, and the encoded output 221 is formatted into packets 231 by data packetizer 230. Transmitter processor 235 controls the interactions of encoder 220 with program memory 225, and also provides the necessary control information so as to form packets 231. Packets 231 are transmitted via packet network 70 and detected by an access device (e.g. 30) where the packets are processed by data extractor 250 of the access device to produce the received counterpart 251 of compressed output 221 in transmitter 201. The resulting data stream 251 is decompressed and decoded by decoder 260 to produce received frame 211 corresponding to the content provided in frame 210.

**[0020]** In the exemplary embodiment depicted herein, data packetizer 230 generally includes elements corresponding to the MPEG-2 standard, for generating: (a) an elementary stream (ES) of encoded video; (b) a packetized elementary stream (PES) from the elementary stream; and (c) a transport stream from one or more PESs to derive the MPEG-2 packets 231 ready for transport over network 70. The encoded video is processed by adding information that is used to reconstruct the frames at the receiving end. Such information includes, for example, timing information (e.g., the Presentation Time Stamp (PTS) and the Decode Time Stamp (DTS)) , clock reference information (e.g. PCR) and PMT/EIT data. Thus, in a generic sense, data packetizer 230 transforms the encoded video to the transport stream which contains all necessary information to re-transform the transport stream to derive the content.

**[0021]** In the home network system illustrated in FIG. 1, one or more of the access devices (20, 30, 40, 50, 60) is operable for both receiving content transmitted via an MPEG-2 transport stream and also operable for transmitting or re-distributing the content to another device which resides either within home network 70 or external to the network. Such transmission is accomplished using a "protocol stack" comprising "applications/service" level layer application for producing the encoded MPEG-2 audio/video/data stream packet; "transport" level layer applications for encapsulating each packet in the MPEG-2 stream by appending headers (e.g. RTP, UDP headers); "Network" level layer applications for further encapsulating the prior layer by appending the IP header information, including for example, routing or re-routing information. "Data Link" level layer applications accomplishes error control and access control and further encapsulates the resulting packets by appending an Ethernet header for instance. "Physical" level layer applications engender the actual transmission at the bit-level.

[0022] In one configuration, the access device 30, in addition to the receiving function shown therein, would also include each of the functional elements illustrated in the transmitter portion 201 of FIG. 2 for transmitting and/or re-distributing content received in the transport stream to another device.

[0023] In accordance with an aspect of the present invention, when an access device within a home network receives a terrestrial broadcast signal as described above, the device may be functionally capable of distributing the content contained in the broadcast signal to another device, either within the network or outside the network via a home router. Nevertheless, it may be desired to place certain restraints on the re-distribution of such content to other devices outside of the home network, based on the nature of the content, for example.

[0024] According to an aspect of the present invention, functionality provided within the access device itself at the software application level operates to determine whether the content is to be distributed outside the network (based on a flag contained in a portion of the transport stream packets), without requiring modification to the infrastructure of the home network environment.

[0025] In present home network configurations a home router may be configured to perform Network Address Translation (NAT) as described in RFC 3022, for example. The router receives a packet and examines the packet's destination IP address. Based on the subnet mask and its own local IP address, the router determines whether the packet is intended for the home network or whether it is intended for a destination device outside of the home network. If the packet is intended for a destination outside of the home network, the router forwards the packet to an external address after substituting its own public IP address into the packet's source IP address field. When the destination device responds, it responds back to the public IP address of the router. The router receives the response and maps it to the request, thereby determining which device inside the home network made the original request. The router places the destination device's local IP address into the destination field and forwards it on to the originating device.

[0026] In accordance with the configuration shown in FIG. 1, each device on an Ethernet network has a physical address and an IP address. As shown in FIG. 3, in an exemplary embodiment, terrestrial broadcast signal 300 comprising an MPEG-2 transport stream intended for access device 30 (FIG. 1) within home network 70 includes a header/payload pair, namely, header 301 and its accompanying payload 302, header 303 and

its accompanying payload 304, and so forth. Header 301 is generally four-bytes long, and payload 302 is 184-bytes. Transport stream 300 is emitted by data packetizer 230 of FIG. 2. Each header contains various header information including PID (Packet Identifier) field data. In addition, the payload is composed of components of the compressed video (or in other applications, audio, data, and teletext/closed captioning), as well as referencing information. Payload 302 includes Program Association Table (PAT) information, which associates a PID with a given program or collection of streams within a common timebase, and Program Map table (PMT) information, which provides more detailed referencing information to further define the mapping between the encoded video stream and the actual packets prepared for transmission, and is used at the receiving end to properly decode the Transport Stream. FIG. 4A illustrates an exemplary configuration linking a given PID 110 to the corresponding PAT 320 and PMT 420.

**[0027]** PMT 420 lists, as identified by row, the Stream Identifier, the Type of signal (e.g., video, audio, data), a PID assigned to that type by the source, and an authorization field 430 such as a broadcast flag (BF) or redistribution control descriptor carried in the video broadcast stream for the purpose of signifying information to downstream applications relating to authorization for the redistribution of content in the stream. In one embodiment, the broadcast flag (BF) is a single bit within the PMT field of the MPEG-2 transport stream, as shown in FIG. 4A. However, additional numbers of bits may be used, for example, to communicate additional information for processing by the access device.

**[0028]** According to a predefined convention, a BF bit value "0" indicates that the content within the transport stream packet is authorized for re-distribution to devices outside the home network (i.e "transport mode"). Conversely, a BF bit value "1" indicates that the content within the transport stream packet is not authorized for re-distribution outside the home network (i.e "inhibit mode").

**[0029]** Alternatively, another field within the broadcast stream, such as the Event Information Table (EIT) 450 shown in FIG. 4B, may include the broadcast flag (BF) for determining authorization. FIG. 4B illustrates an exemplary EIT showing a broadcast start time and a broadcast duration of the object program (PID), along with the BF flag indicating authorization for re-distribution. The EIT may be multiplexed in the transport stream for reception and decoding by the access device. One exemplary implementation may include the BF flag in both the EIT and PMT for terrestrial broadcasts, while, for example, for cable

transport, the BF flag shall be present in the PMT, and, when the EIT is carried, in the EIT, according to a given protocol (e.g. ATSC standard). The BF may appear periodically within the transport stream.

**[0030]** According to an aspect of the present invention, when an access device receives the broadcast signal and decodes the transport stream, the device parses the PMT/EIT field and determines the status of the BF flag 430 indicative of whether the content is authorized for re-distribution outside the home network. A software application module or hardware circuitry may be configured to examine the received payload data to recover the BF flag based on its corresponding table entry and location within the transport stream.

**[0031]** In conjunction with the home network system of FIG. 1, there is shown in FIG. 5 a method for carrying out the present invention of inhibiting unauthorized re-distribution of content according to an exemplary embodiment. When access device 30 (Fig. 1) is connected to home Ethernet network 70 and operable to both receive incoming audio/video/data broadcast streams (step 500) and to retransmit or redistribute the content contained therein, the access device, prior to redistributing the received content, performs the following acts.

**[0032]** The access device obtains location information associated with gateway/router 90 by performing an ARP (address resolution protocol) on the router IP address to obtain the physical address of the router (step 505). The physical address is then stored in memory (step 510). The content intended to be transmitted to a destination device in the form of a packet is then formatted (steps 515, 520) in accordance with predefined format and convention. The access device broadcasts a request for location information for the destination device (step 525) to which the content from the access device is intended to be transmitted to. This may be accomplished by broadcasting an ARP for the destination IP address to obtain the physical address of the destination device. If the destination device is on the home network, the destination device will respond to the access devices request by providing its physical address to the access device.

**[0033]** When router 90 receives the broadcast ARP message, the router determines if the destination IP address is in the local subnet by comparing the portion of the address masked by the subnet mask with the portion of its own address masked by the same subnet mask (step 530). If the router determines that the destination device is outside the local network, the router returns its own physical address for the requested remote destination IP address (step 535).

[0034] The access device 30 receives the response to its request for location information for the destination device (step 540) and compares the physical address returned in response to the ARP (step 525) with the physical address of the router 90 that was previously stored in memory (step 505). If the physical address returned is the same as the gateway address stored in memory (step 545) then the packet to be transmitted is destined for a device outside of the local home network. In this case, the access device then parses the PMT payload field to recover the broadcast flag and determine whether the flag is set (step 550). If the flag is set (indicative of content not authorized for external network distribution) the access device discards the packet (step 555) and awaits the next data packet to format and process (step 515)

[0035] In the case where the broadcast flag in the transport stream packet is not set (step 550), the access device finishes formatting the packet and transmits the packet to the router 90 for routing the content to the destination device outside the home network (step 560). The access device also completes packet formation and transmission to the destination device directly upon determination that a physical address returned in response to the ARP broadcast is different than the physical address associated with router 90 (steps 540, 545), indicating that the destination device is within the home network and thus authorized for redistribution within a local environment.

[0036] The present invention is embodied in machine executable software instructions within the access device, and the present invention is carried out in a processing system by a processor executing the instructions. In other embodiments, hardwired circuitry may be used in place of or in combination with software instructions to implement the present invention. The computer instructions embodying the present invention may be loaded into memory from a persistent store such as a mass storage device and/or from one or more other computer systems over a network. For example, execution in some embodiments that downloaded instructions may be directly supported by the microprocessor and directly executed by the processor. Alternatively, the instructions may be executed by causing the microprocessor to execute an interpreter that interprets the instructions by causing the microprocessor to execute instructions, which convert the instructions into a format that can be directly executed by the microprocessor. Thus, the present invention is not limited to any specific combination of hardware circuitry and software, nor to any particular source for the instructions executed by the access device.

[0037] As described in the above exemplary embodiments, the present invention exploits the difference between an IP address on the local network and an IP address outside the local network wherein the distinction between the address spaces may be determined by subnet masks and gateway addresses. The present invention implements a mechanism for inhibiting the unauthorized redistribution of content by parsing packet information within the transport stream and determining whether the broadcast flag is set, whereby the application shall not forward the content to an IP address that is outside of its local subnetwork as defined by the subnet mask and gateway addresses.

[0038] Although the invention has been described in terms of exemplary embodiments it is not limited thereto. For example, as an added level of security, the home network may use non-routable IP addresses (i.e. private addresses). That is, certain IP addresses are reserved according to predetermined standards and conventions such as the IETF standard. The mapping table associated with Internet routers (i.e. those devices within internet 100 of FIG. 1) would thus not include these non-routable addresses. Accordingly, in the event that unauthorized content is inadvertently distributed outside of the home network, those routers receiving this information would be unable to forward it to its intended destination (as this is a non-routable address) and therefore drop the packetized data. If additional protection is desired, authentication mechanisms and encryption protocols may be utilized to provide further security and guard against unauthorized access and redistribution of certain protected content. The access device that intends to forward the content over the home network would then be required to ensure that the application that it would like to forward the content to is a trusted and compliant application. Alternatively, the access device can be configured to package the content into an IP stream using a different packing format according to a predefined convention that would be recognizable only to compliant devices.

[0039] Although the invention has been described in terms of exemplary embodiments, it is not limited thereto. For example, although the present embodiment is described with reference to an access device that is able to receive digital signals from a broadcast source such as, but not limited to, terrestrial broadcast source, a cable system, it is clear that the above described method of controlling the distribution of digital signals can be used with any device attached to a network, such as a home network. The appended claims should be construed broadly to include other variants and embodiments of the invention, which may be made by those skilled in the art without departing from the scope and range of equivalents of the invention.